REMARKS

Applicant has carefully reviewed and considered the Office Action mailed on August 13, 2003, and the references cited therewith.

Claims 1-45 remain pending in this application.

§103 Rejection of the Claims

Claims 1, 2, 4, 5, 8, 18 and 19 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,324,656) in view of Ptacek et al. (U.S. Patent No. 6,343,362).

Gleichauf describes a system and method for characterizing a network and identifying vulnerabilities. As noted by the Examiner, Gleichauf discloses a network configuration module having network configuration data. In contrast to Applicant, however, Gleichauf identifies and tests vulnerabilities by applying a rule set (col. 4, lines 43-47, col. 7, lines 6-31 and Fig. 4) to identify vulnerabilities and then testing the actual network to see if the vulnerabilities exist.

Applicant teaches that it can be difficult to test vulnerabilities on the network itself. As noted on p. 1, lines 28-30, such tests can disrupt the network and may leave footprints such as event log entries and the like on scanned machines. Therefore, in contrast to Gleichauf, Applicant teaches the use of a separate simulator to identify and test vulnerabilities.

The Examiner stated that Gleichauf discloses a security modeling system having a network configuration module and a network vulnerabilities database but that Gleichauf does not disclose a network simulation. The Examiner stated that Ptacek "discloses a network simulation for analyzing attacks against a network." Applicant disagrees.

Ptacek describes a higher-level computer language that can be used to create programs that simulate attacks against a computer network. Ptacek notes the difficulty network administrators face in generating the network traffic needed to test their network for known vulnerabilities. As noted at col. 2, lines 6-41, although the vulnerability may be easily explained, generating it in order to test your system can be complex and time consuming.

> As a result, security professionals are forced to spend valuable time fishing through hacker-exploit code to find poorly-written Linux programs that do not even compile. This time could be better spent quickly writing the equivalent in portable, simple CASL code, which will not only run on the machines they need to run on, but also work exactly how they need to work.

> Attempting to write these programs using existing programming languages, such as the "C" programming language, is not practical. While security tools may certainly run a bit faster if hand-coded in "C", the runtime speed benefits are probably not outweighed by the development speed costs. A "C" programmer needs to worry about memory allocation, portable network I/O, and several other issues ranging from error handling to byte ordering.
>
> What is needed is a system that allows the system administrator or the programmer to focus on network security programs--what is happening on the network--and not worry about issues attendant to conventional programming environments, such as C. Such a system should facilitate the task of testing network security by providing methodology that allows a user (administrator) to develop test programs without having to build network packets (i.e., communication-protocol packets) or otherwise write raw network code. The present invention fulfills this and other needs.

Ptacek, col. 2, lines 26-52. Ptacek then goes on to describe the language used to generate network traffic used to test the network for known vulnerabilities. Ptacek does not, therefore, describe a network simulation for analyzing attacks against a network, but instead describes a computer language for generating attacks against the network itself.

Since neither reference describes "a simulator coupled to the network configuration module to simulate and analyze networks based on the network configuration data" as described by Applicant and claimed in claims 1-8, claims 1-8 are patentable over the cited references. Reconsideration of claims 1-8 is respectfully requested.

Similarly, since neither reference describes "simulating the network based on the network configuration" or "determining vulnerabilities of the simulated network using the vulnerability information stored in the database" as described by Applicant and claimed in claims 18-27, claims 18-27 are patentable over the cited references. Reconsideration of claims 18-27 is respectfully requested.

Claims 3 and 6 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,324,656) in view of Ptacek et al and in further view of Gleichauf et al. (U.S. Patent No. 6,282,546, hereinafter "G2").

G2 describes a system and method for characterizing a network and recording intrusion events occurring against the network. At col. 3, lines 28-62, G2 states that "one of the more effective ways to deal with a network administrator's requirements is to store network information in a multi-dimensional database that fully represents the managed network

environment. The multi-dimensional database can then support flexible query techniques against the stored data such as slices, pivoting, zooming and drill down." While G2 does describe the use of a database, he does not describe the use of a simulator having a network vulnerabilities database used to simulate and analyze networks based on the network configuration data as describe by Applicant and claimed in claims 3 and 6. Reconsideration of claims 3 and 6 is respectfully requested.

Claim 7 was rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,324,656) in view of Ptacek et al (U.S. Patent No. 6,343,362) and in further view of Sparks, II (U.S. Patent No. 6,352,479). Claim 7 is dependent on claim 1 and is patentable over the cited references for the reasons discussed for claim 1 above.

In addition, the Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). To do that the Examiner must show that some objective teaching in the prior art or some knowledge generally available to one of ordinary skill in the art would lead an individual to combine the relevant teaching of the references. *Id.*

The *Fine* court stated that:

> Obviousness is tested by "what the combined teaching of the references would have suggested to those of ordinary skill in the art." *In re Keller*, 642 F.2d 413, 425, 208 USPQ 871, 878 (CCPA 1981)). But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." *ACS Hosp. Sys.*, 732 F.2d at 1577, 221 USPQ at 933. And "teachings of references can be combined *only* if there is some suggestion or incentive to do so." *Id.* (emphasis in original).

The M.P.E.P. adopts this line of reasoning, stating that

> In order for the Examiner to establish a *prima facie* case of obviousness, three base criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure.

M.P.E.P. § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir. 1991)).

In addition, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP § 2143. The Examiner must avoid hindsight. *In re Bond*, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990).

Applicant notes that, even if, for argument's sake, Sparks describes an attacker and a defender in the context of an Internet-based game, there is no teaching or motivation in any of the cited references to create an environment where an attacker can attack a computer network through a simulation of that network and a defender defend that same simulated network. Applicant respectfully submits that the Office Action relied on the Applicant's disclosure and/or impermissible hindsight in forming the rejection of claim 7 over the cited references. As such, Applicant respectfully requests that this rejection be withdrawn.

Claim 9 was rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,324,656) in view of Ptacek et al and in further view of Sparks, II.

Once again, even if, for argument's sake, Sparks describes an attacker and a defender in the context of an Internet-based game, there is no teaching or motivation in any of the cited references to create an environment where an attacker can attack a computer network through a simulation of that network and a defender defend that same simulated network. Applicant respectfully submits that the Office Action relied on the Applicant's disclosure and/or impermissible hindsight in forming the rejection of claim 9 over the cited references. As such, Applicant respectfully requests that this rejection be withdrawn.

Claims 10, 11, 13, 14, and 16 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,324,656) in view of Ptacek et al and in further view of Bergman et al. (U.S. Patent No. 6,422,694) and in futher view of Smith, Jr. (U.S. Patent No. 5,662,478). Claims 12 and 15 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,324,656) in view of Ptacek et al and in further view of Bergman et al. and in futher view of Smith, Jr. and in further view of Gleifhauf et al. (U.S. Patent No. 6,282,546).

As noted above, neither the Ptacek reference nor the two Gleighauf references disclose the use of a simulator to simulate a computer network for security modeling. This feature is

described by Applicant and claimed in claims 10-17. Applicant is unable to find any teaching of this feature in either Bergman or Smith. Reconsideration of claims 10-17 is respectfully requested.

Claim 17 was rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,324,656) in view of Ptacek et al and in further view of Bergman et al. and in further view of Smith, Jr. and in further view of Sparks, II.

As noted above, neither the Ptacek reference nor the two Gleighauf references disclose the use of a simulator to simulate a computer network for security modeling. This feature is described by Applicant and claimed in claims 10-17. Applicant is unable to find any teaching of this feature in either Bergman, Smith or Sparks. Reconsideration of claim 17 is respectfully requested.

Claim 20 was rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S Patent No. 6,324,656) in view of Ptacek et al and in further view of Ballard et al. (U.S. Patent No. 4,937,825). Claim 20 is dependent on claim 18 and patentable for the reasons given in discussing claim 18 above.

Claims 21, 22, 23, and 26 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S Patent No. 6,324,656) in view of Ptacek et al and in further view of Jackson (HACKER, The Computer Crime Card Game). Claims 21, 22, 23, and 26 are dependent on claim 18 and patentable for the reasons given in discussing claim 18 above.

Gleichauf and Ptacek are discussed above. As noted above, neither reference describes "simulating the network based on the network configuration" or "determining vulnerabilities of the simulated network using the vulnerability information stored in the database" as described by Applicant and claimed in claims 18-27.

Jackson describes a card game based on the Illuminati system. The card game uses hacker terminology to create a game in which players try to game access to one or more cards representing computer systems. It's the Examiner's position that Jackson discloses mission objectives when he states that a player wins by gaining access to a given number of systems. The game described by Jackson builds a network during game play by laying cards down in a domino-like manner. There is no "simulating the network based on the network configuration" or "determining vulnerabilities of the simulated network using the vulnerability information

stored in the database" as described by Applicant and claimed in claims 21, 22, 23 and 26. Furthermore, there is no "simulating the network based on the network configuration and mission objectives." Reconsideration of claims 21, 22, 23 and 26 is respectfully requested.

Claims 23, 24, and 25 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S Patent No. 6,324,656) in view of Ptacek et al and in further view of Jackson and in further view of Kurtzberg et al. (U.S. Patent No. 5,961,644).

Gleichauf, Ptacek and Jackson are discussed above. As noted above, none of the references describe "simulating the network based on the network configuration" or "determining vulnerabilities of the simulated network using the vulnerability information stored in the database" as described by Applicant and claimed in claims 18-27.

Kurtzberg, like Ptacek, describes launching simulated attacks on the network itself, instead of a simulation of the network based on a network configuration. See Kurtzberg, col. 3, lines 42-50. Kurtzberg, therefore, does not disclose "simulating the network based on the network configuration" or "determining vulnerabilities of the simulated network using the vulnerability information stored in the database" as described by Applicant and claimed in claims 18-27. Furthermore, Kurtzberg does not, as the Examiner states, disclose dynamically interacting with an attacker. Kurtzberg describes a test system which is the attacker. Reconsideration of claims 23, 24 and 25 is respectfully requested.

Claim 27 was rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S Patent No. 6,324,656) in view of Ptacek et al and in further view of Jackson and in further view of Gleichhauf et al. (U.S. Patent No. 6,282,546).

None of the cited references can teach updating the vulnerabilities database based on the results of a simulation of the network since none of them teach running a simulation of a network. Reconsideration of claim 27 is respectfully requested.

Claim 28-30 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S Patent No. 6,324,656) in view of Johnson (Simulated Attack for Real Network Security) and in further view of Kurtzberg et al. and in further view of Jackson.

Gleichauf, Ptacek, Kurtzberg and Jackson are discussed above. As noted above, none of the references describe "simulating the network based on the network configuration" or "determining vulnerabilities of the simulated network using the vulnerability information stored

in the database" as described by Applicant and claimed in claims 18-27. Instead, Ptacek and Kurtzberg describe simulating an attack. Johnson does the same. This is a fundamental difference over the method described and claimed by Applicant. As noted above, Applicant teaches that it can be difficult to test vulnerabilities on the network itself. As noted on p. 1, lines 28-30, such tests can disrupt the network and may leave footprints such as event log entries and the like on scanned machines. Therefore, in contrast to the multitude of references cited by the Examiner, Applicant teaches the use of a separate simulator to identify and test vulnerabilities.

Reconsideration of claims 28-30 is respectfully requested.

Claims 31-33 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S Patent No. 6,324,656) in view of Johnson and in further view of Kurtzberg and in further view of Jackson and in further view of Porras et al. (6,321,338).

None of the references describe network simulation; some disclose simulated attacks on a network. Porras provides no greater teaching of a graphical user interface in this context than does Ptacek in the rejection of claim 5 above. If anything, Porras appears to be less relevant to a method of opposing network attackers. Porras does describe calculating a security score but that scoring is in the context of tracking actual network traffic, not traffic on a simulated version of the network. Reconsideration of claims 31-33 is respectfully requested.

Claims 34-38 and 40-42 were rejected under 35 USC § 103(a) as being unpatentable over Johnson in view of Porras et al and in further view of Gleichhauf et al. (U.S. Patent No. 6,282,546).

As noted above, Johnson describes a simulated attack on an existing network. Porras describes monitoring an existing network for suspicious traffic. G2 describes a database used to store information on network vulnerabilities. None of the references disclose "a simulator having a plurality of databases" used to simulate objective networks as described by Applicant and claimed in claims 34-38 or "simulating the network based on the network configuration" and "determining vulnerabilities of the simulated network" as described by Applicant and claimed in claims 40-42. Reconsideration of claims 34-38 and 40-42 is respectfully requested.

Claim 9 was rejected under 35 USC § 103(a) as being unpatentable over Gleichauf et al. (U.S Patent No. 6,324,656) in view of Ptacek et al and in further view of Jackson.

Gleichauf, Ptacek and Jackson are discussed above. As noted above, none of the references describe game having a simulator which simulates and analyzes networks based on the network configuration and a network vulnerabilities database as described by Applicant and claimed in claims 9, 38 and 39. Reconsideration of claims 9 and 38 is respectfully requested. Applicant notes that there was no rejection of claim 39 in this Office Action and respectfully submits that claim 39 is patentable for the reasons given for claims 9 and 38 above.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and reconsideration and notification of allowance of all pending claims is earnestly requested. The Examiner is invited to telephone Applicant's attorney (612) 373-6909 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743

Respectfully submitted,

ALAN DOWD ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6909

Date January 13, 2004 By Thomas J. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 13 day of January, 2004.

Gina M. Uphus
Name

Gina Uphus
Signature